

# Vordel XML Gateway

Apply control to Web and SOA applications

---

Vordel XML Gateway applies control to Web and SOA applications by enforcing policies over traffic on the network. It also protects applications from malicious attack, allowing them to be deployed in safety and confidence.

XML validation and threat-scanning is performed at wire-speed by the Vordel XML Gateway, allowing applications to run safer and faster.

Vordel XML Gateway forms an integral component of any enterprise SOA infrastructure and can be deployed as part of a strategic architecture of Enterprise Service Buses, Enterprise Management, Identity Management and runtime Governance products.

## Distributed Policy Enforcement with Centralized Management

Vordel XML Gateway performs the runtime enforcement of policies defined in Governance products such as Oracle WSM (Web Services Manager) and Oracle Enterprise Manager. The WS-Policy standard is used to allow policies to be centrally defined in Oracle infrastructure and then enforced at multiple points on the network by Vordel XML Gateway infrastructure.

### Powerful rules engine

Powerful rules engine

An intuitive policy management console enables administrators to add security and management policies to multiple gateway devices. Rules may include significant complexity such as branching (“if the message is from this particular sender, then validate it against this particular schema”).

Rules are defined to be independent of the resources which are being protected by the Vordel XML Gateway.

### Enforce Triple-A (Authentication, Authorization, Accounting) rules

Vordel XML Gateway can apply identity policies defined in Identity Management products and apply them to Web and SOA traffic. These rules include authentication, authorization and Single Sign-On. Vordel currently supports Oracle Access Manager, Oracle Internet Directory, LDAP, Microsoft Active Directory, CA SiteMinder, Entrust GetAccess, IBM Tivoli Access Manager, and RSA Access Manager, as well as other IM products.

### Security for all flavors of XML applications

Vordel XML Gateway provides protection for all three classes of XML applications: SOAP-based Web Services, “plain XML” applications which do not use SOAP, and “REST style” applications which are invoked using HTTP GET.

This protection includes Web 2.0 applications which make use of the XHR (XMLHttpRequest) object.

### Comprehensive XML Firewalling

Vordel XML Gateway provides full threat protection against XML attacks and sends email alerts to security administrators. Untrusted service invocations are denied by default. XML applications are protected using a comprehensive set of pre-built content-filtering and traffic-analysis rules. Some of the common attacks it protects against include:

- Clogging attacks
- Service Scanning
- Covert channel attacks
- XML Denial of Service
- Data-harvesting attacks
- XML threats such as SQL Injection and XML Denial of Service
- Protect against vulnerabilities associated with XML parsers, including under both .Net and Java frameworks
- Blacklisting with Network Firewalls

### Data Integrity control checks

Validate incoming XML and SOAP messages for conformance with XML Schemas, WS-I Basic Profile data integrity.

### Client Authentication

Perform authentication on clients using industry standard HTTP Authentication and X.509 Certificates with SSL. This is in compliance with the WS-I Basic Security Profile. Vordel also supports Kerberos, SAML and WS-Security to authenticate users and applications.

## Traffic throttling

Vordel XML Gateway protects Web Services from unanticipated traffic spikes, by smoothing out the traffic. It also limits clients to agreed Web Service consumption levels in accordance with service usage agreements. This allows Vordel's customers to charge their clients for different levels of Web Services usage.

## Service Virtualization

Vordel XML Gateway serves as an important control point for XML traffic on the network. By shielding end point Web Services from direct access, the gateway allows for the virtualization of these services, and clients access the XML Gateway as if it was the Web Service itself. This allows different "views" of Web Services to be presented to different clients.

## Cloud Ready

Vordel XML Gateway can be deployed in the cloud or can mediate between externally and internally hosted applications. Use Vordel XML Gateway to:

- Control the use of the cloud
- Monitor cloud service availability and responsiveness using Service Level Agreements
- Safeguard and classify confidential data
- Conserve network bandwidth and increase performance and decrease costs
- Control access between the organization and the services hosted in the cloud
- Audit and archive interactions with the cloud services
- Secure data transfer between onsite and offsite application environments

## Rapid Deployment

Vordel provides pre-built policies which allow Vordel's customers to get up-and-running quickly. The gateway includes many features which speed up deployment. For example, certificates and private keys, necessary for many XML security functions, may be issued on-board. The device has a "Deny by Default" defense posture, in order to detect and block any unauthorized deployments of Web Services. Policies can be re-applied across multiple application endpoints using simple drop-down menus.

## Audit trail

Maintain an audit trail of all internal and external XML-based communications in a tamper-proof store. Facilitate privacy compliance support by allowing de-identification: that is, allowing sensitive information, such as customer names, to be encrypted or stripped out of XML traffic.

## Real Time Monitoring

Vordel XML Gateway ships with a real-time Monitoring Console that provides color-coded message filtering status on message throughput. Administrators can search events on a per message or event type (e.g. Schema validation).

## Processing Offload for Application Acceleration

Offload the heavy-lifting of XML from application servers and onto the network. XML operations such as XML Schema Validation and XSLT are notoriously slow. The gateway uses patented, wirespeed, acceleration to speed these tasks. This frees up resources on application servers and allows applications to run faster.

## XML Data Enrichment

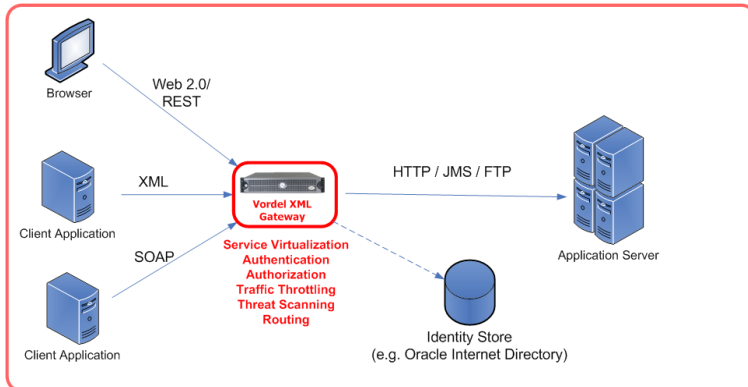
Automatically populate content in XML documents from sources such as databases. By putting this functionality onto XML Networking infrastructure, the information is automatically populated into the XML messages before they reach the consuming Web Services. This simplifies and accelerates applications in ESBs or Application Servers.

## Supported platform

Vordel XML Gateway is available as a hardware appliance; as software for Windows, Linux, and Solaris; as a VMWare appliance and as an Amazon EC2 Cloud AMI.

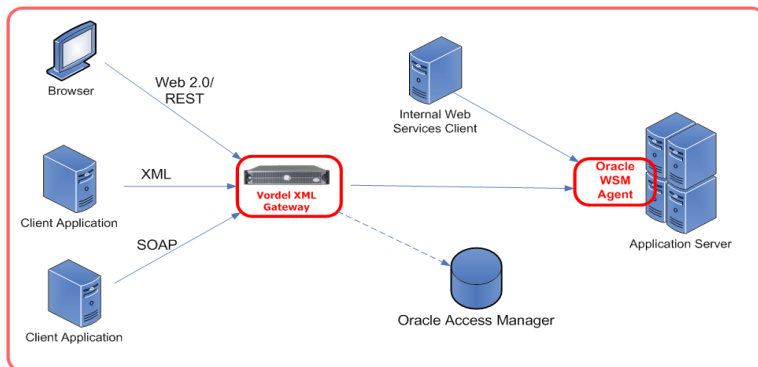
## Deployment

The following diagram shows the Vordel XML Gateway deployed to manage traffic from Web applications, XML, and SOAP. The Vordel Gateway comes with an onboard identity store, but may also be used with an external identity store such as the Oracle Internet Directory shown in the diagram below.

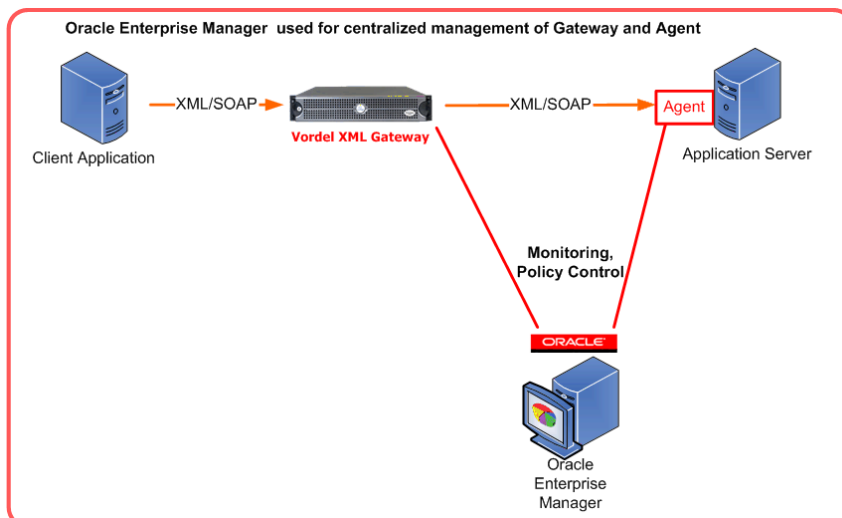


## Deployment with Oracle Infrastructure

The following diagram shows the Vordel XML Gateway performing authentication and authorization on the network, through its built-in connector to Oracle Access Manager. Additionally, at the Web Service endpoint, an Oracle WSM Agent may be used to perform fine-grained authorization, based on a security token placed into the message by the Vordel XML Gateway.



Oracle Enterprise Manager may be used to monitor and control the Vordel XML Gateway, as shown in the following diagram. The metrics on Web Services usage which is gathered from the Vordel XML Gateway are displayed by the Oracle Enterprise manager.



## Performance Optimized VX Deployment Platform

Integrated into the firewall is Vordel's patented core VXA (Vordel XML Acceleration) engine. This processing engine accelerates XML processing. The VX deployment platform also includes cryptographic acceleration hardware embedded in the device and Gigabit Ethernet cards provide wirespeed network performance.

## Supported Standards

Oracle integrations/interoperability	Oracle Access Manager, Oracle Application Server 11g, Oracle BPEL Process Manager, Oracle EDI B2B Gateway, Oracle Enterprise Manager, Oracle Internet Directory, Oracle 8,9,10,11 Database, Oracle Linux
Web Services Protocols	SOAP 1.1 & 1.2 , Plain XML (POX), REST, Web 2.0 (XMLHttpRequest, JSON)
Networking	Service Virtualization, Content-based routing, Source-based routing, Identity-based routing, Protocol Conversion, XML Data Enrichment
Transport Protocols	HTTP 1.0 & 1.1, JMS, MQ, FTP, SFTP, TIBCO Rendezvous, TIBCO EMS, SMTP, POP, TCP
Service Governance	WSDL 1.2, WS-Policy 1.2, WS-SecurityPolicy 1.1, WS-Policy Attachment, UDDI
Policy Control	Drag-and-drop policy creation, Conditional branching within policies, Standards-based Import/Export of policies, Policy chaining, Policy Migration, Wildcard values within policies, Distributed Policy Enforcement with Centralized Management
Identity Management Integration	Oracle Access Manager, Sun Access Manager, Novell Access Manager, CA SiteMinder, RSA Access Manager, Entrust GetAccess, IBM Tivoli Access Manager, XACML
LDAP	Oracle Internet Directory, Sun, Novell, Siemens, Microsoft Active Directory
Security and Identity Mediation	Built-in Security Token Service (STS), SAML Token Issuance and Injection, WS-Trust, Credential Mapping, Token mapping (X.509 to SAML, Kerberos, etc),
Encryption and Signing	SSL, XML Encryption, XML Signature, WS-Security SOAP Message Security, Threat Detection
XML Firewalling	XML Entity Expansion and Recursion Attacks, XML Document Size Attacks, XML Document Width Attacks, XML Document Depth Attacks, XML Wellformedness based Parser Attacks, Jumbo Payloads, Recursive Elements, MegaTags – aka Jumbo Tag Names, Public Key DoS attack, XML Flood, XML Encapsulation, XML Virus, Replay Attacks, Resource Hijack, Dictionary Attack, Message Tampering, Falsified Message, Data Tampering, Message Snooping, XPath Injection, SQL Injection, XPath Injection, Xquery Injection, WSDL Enumeration, Routing Detour, Schema Poisoning, Malicious Morphing, Malicious Include – also called XML External Entity (XXE) Attack, Memory Space Breach, XML Morphing, Parameter Tampering, Coercive Parsing, Field level validation, Scanning outgoing messages for sensitive content based on metadata or Regular Expression Pattern, WSDL Scanning, XML Bomb Attacks, Rogue SOAP Attachments, Detect viruses in SOAP Attachments, Schema Validation, XML Clogging Detection, SOAP Operation Filtering, IP Address Filtering, Traffic Throttling, HTTP Header Analysis, HTTP Query String Analysis, Malicious content signature library
Authentication	Kerberos, HTTP Authentication (Basic/Digest), SSL Mutual Authentication, WS-Security 1.1 & 1.0, WS-Security UsernameToken, WS-Security X.509 Certificate Token, WS-Security Kerberos Profile and other types
Authorization	Role-based access control, Authorization based on database query, Content-based authorization, Delegation to third-party Authorization systems
Audit	Traffic Logging, Log Signing
Monitoring & Alerting	Email, SNMP, Syslog, Windows Event Log, CheckPoint OPSEC, Embedded real time message monitor, Oracle Enterprise Manager, Adobe Flash Web-based monitoring
Extensibility	JavaScript API for custom filters, Java API for custom filters, Conversion, XSLT, Custom Java Message Conversion
Service Quality	Service outage detection, Service Level Agreement monitoring
Certificate Management	X.509 Certificate Issuance, Certificate Revocation List (CRL), OCSP, XKMS, Certificate chaining
Data Integration	Oracle 8,9, 10 & 11 Database, Mysql, Microsoft SQL Server, JDBC
Anti-Virus	Sophos, ClamAV
Appliance Specification	2 x PE1950 Quad-Core Xeon X5460 3.16GHz/2x6MB 1333FSB, 4GB FB 667MHz, 2 x 500GB SATA2 Universal (7,200 rpm) in RAID configuration, nCipher nFast 4000, 670W hot-plug redundant power supply, 2 x Broadcom® NetXtreme 5721 Single Port Gigabit Ethernet NIC, Management Network Interface
Appliance Form	1U Rack-mountable chassis 30.4" (77.2cm) D x 16.7" (42.6cm) W x 1.67" (4.26cm) H with bezel attached Rack Weight 35.8 lbs (16.3 Kg)
Appliance Environmental Characteristics	Operating Temperature: 10° C to 35° C (50° F to 95° F) Storage Temperature: -40° C to 65° C (-40° F to 149° F) Operating Relative Humidity (non-condensing twmax=29C): 20% to 80% non-condensing Maximum humidity gradient: 10% per hour, operational and non-operational conditions Storage Relative Humidity: 5% to 95% non-condensing (twmax=38C) Operating Vibration: 0.26G at 5Hz to 350Hz for 2 minutes Storage Vibration: 1.54Grms Random Vibration at 10Hz to 250Hz for 15 minutes Operating Shock: 1 shock pulse of 41G for up to 2ms Storage Shock: 6 shock pulses of 71G for up to 2ms Operating Altitude: -16 to 3,048m (-50 ft to 10,000 ft) Storage Altitude: -16m to 10,600m (-50 ft to 35,000 ft)
Operating System Support Matrix	Windows 7, Windows Vista, Windows XP, Windows Server 2003, Windows Server 2008, Red Hat Linux, Suse Linux ES, Ubuntu Linux, Debian Linux, Solaris 10 Sparc, Oracle linux
Extensibility	Java, ECMA JavaScript, XSLT
STS	Built-in Security Token Service (STS)

### Ireland

Vordel  
30 Pembroke street upper  
Dublin 2  
Tel: +353 1 234 2500

### Washington

Washington DC Metro Headquarters  
13800 Coppermine Rd. #306  
Herndon, VA. 20171  
USA  
US Sales 1-(866)-460-0987

### Boston

125 Metropolitan Avenue  
Boston, MA 02131  
USA  
US Support 1-(866)-607-0023

### UK

1st Floor Holborn Gate  
330 High Holborn  
London WC1V 7QT  
United Kingdom  
Tel: +44 207 849 6885

Vordel White Paper, Copyright © 2000 – 2009 Vordel Limited. All rights reserved. All content in this datasheet is for general information and promotional purposes only and neither constitutes a technical specification nor an offer to enter into contractual relations with Vordel or with any other party; and Vordel reserves the right to alter such content without notice at any time. The trademarks, logos and service marks displayed herein are registered and unregistered trademarks of Vordel and others.